UCRL-TB-122805

ASP Offers You ...

A highly skilled staff of computer security and product development specialists with expertise in:

Distributed Systems Development

Unix, VMS and Small Systems

User Interfaces

Portability Issues

Vendor Collaboration

Firewall Capabilities

Operating System Vulnerabilities

Network Monitoring and Analysis

Public Key Cryptography

Text Analysis

For Additional Information ...

If you wish to fund or obtain any of our products or wish to discuss the creation of a new product, please contact:

Doug Mansur, Program Manager

(510) 423-6224
cstc@llnl.gov
http://ciac.llnl.gov/cstc/CSTCProducts.html

Computer Security Technology Center

Lawrence Livermore National Laboratory
PO Box 808, L-303
Livermore, California 94551

(510) 423-6224
(510) 423-8002 (Fax)
Internet: cstc@llnl.gov

Advanced Security Projects

Making Information Safe

Teaming For Information Security ...

ASP Product Portfolio

Advanced Security Projects (ASP) applies its expertise in project development and the computer security field to create state-of-the-art products which enhance the security of information resources.

Working closely with the Computer Incident Advisory Capability (CIAC), ASP has access to the latest threats to computer security. By combining this knowledge with its own expertise and a commitment to reusable code libraries and consistent software engineering, ASP can create innovative solutions to today's security problems in a timely manner.

Teaming For Information Security

There is no single magic bullet for achieving information security. Security products and their developers have to work together cooperatively to improve overall security. We have a long track record of working with others to advance the state-of-the-art of information security. Past and present partners have included Sandia National Laboratories, Sun Microsystems, Texas Instruments, and U.C. Davis.

We continue to seek opportunities to partner for the advancement of information security technology and the application of our products and expertise. Possible partnership projects include large scale research projects for government organizations such as ARPA, cooperative research and development of security products, and arranging technology transfers of our existing products.

Network Intrusion Detector (NID)
The NID system detects and analyzes intrusive network behavior. NID has unique capabilities: completely passive monitoring, no changes to protected hosts, real-time detection, retrospective replay and analysis, network statistics, and evidence gathering activated upon detection of intrusive behavior. NID's intrusion analysis is based upon attack signature recognition, anomaly detection, and a vulnerability risk model.

Security Profile Inspector/Net (SPI-NET)
SPI-NET is a distributed security inspection product for networks of Unix and VMS systems, supporting simultaneous inspection of multiple target systems from a centralized command host, with flexible automated job scheduling and reporting. Digital signatures authenticate and encrypt data traffic. Inspections include system vulnerabilities, passwords, system change detection, and system software authentication testing.

Text Analysis Project (TAP)
TAP analyzes text files for sensitive or classified material by searching for sensitive phrases. TAP is aware of text concepts such as verb conjugation, synonyms, and thesauruses. The user defined searching criteria can be easily adapted to many purposes such as searching for waste, fraud, and abuse; searching for inadvertent classified or proprietary information; pre-scanning text files for transfer to a less sensitive machine; and classifying (or declassifying) documents.

Secure Software Distribution System (SSDS)
SSDS will provide automated analysis, notification, distribution, and installation of security patches and related software to network-based computer systems. SSDS will allow a network administrator to monitor and maintain the software integrity of hundreds of individual systems from a central point through automated means.

UnAuTH
The UnAuTH tool provides a single point of security management for network change detection, unauthorized cross-connect detection, and security validation checks.

Work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.